

An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks

Year: 2023 | Citations: 188 | Authors: Cheolhee Park, Jonghoon Lee, Youngsoo Kim, Jong-Geun Park, Hyunjin Kim

Abstract

As communication technology advances, various and heterogeneous data are communicated in distributed environments through network systems. Meanwhile, along with the development of communication technology, the attack surface has expanded, and concerns regarding network security have increased. Accordingly, to deal with potential threats, research on network intrusion detection systems (NIDSs) has been actively conducted. Among the various NIDS technologies, recent interest is focused on artificial intelligence (AI)-based anomaly detection systems, and various models have been proposed to improve the performance of NIDS. However, there still exists the problem of data imbalance, in which AI models cannot sufficiently learn malicious behavior and thus fail to detect network threats accurately. In this study, we propose a novel AI-based NIDS that can efficiently resolve the data imbalance problem and improve the performance of the previous systems. To address the aforementioned problem, we leveraged a state-of-the-art generative model that could generate plausible synthetic data for minor attack traffic. In particular, we focused on the reconstruction error and Wasserstein distance-based generative adversarial networks, and autoencoder-driven deep learning models. To demonstrate the effectiveness of our system, we performed comprehensive evaluations over various data sets and demonstrated that the proposed systems significantly outperformed the previous AI-based NIDS.